REMARKS

This amendment is responsive to the Office Action dated February 17, 2005. No amendments have been made by way of this communications. Claims 1-22 are pending.

Claim Rejection Under 35 U.S.C. § 103

In the Office Action, the Examiner rejected claims 1-21 under 35 U.S.C. 103(a) as being unpatentable over Maritzen et al. (US Publication No. US2002/0073042) in view of Bolle et al. (US 6,819,219) and Etzel et al. (US 6,577,734). The Examiner further rejected claim 22 under 35 U.S.C. 103(a) as being unpatentable over Maritzen et al. in view of Bolle et al. and Etzel et al. and further in view of Rydbeck et al. (US 6,195,564). Applicants respectfully traverse the rejection.

As a preliminary comment, it appears the Examiner has failed to address certain elements required by these claims. For example, with respect to claim 1, the Examiner failed to address the requirement of a personal digital identifier device that includes a biometric component, and a processor that evaluates whether a template derived from said digital representation corresponds to a master template derived from a user's biometric digital representation previously produced by said biometric component. In other words, claim 1 literally requires that the personal digital identifier device include a biometric component that generates the master template, i.e., that the portable device itself internally generate the master template.

None of the references supplied by the Examiner suggests a personal identifier device that internally generates the master template from the biometric. In contrast, Bolle merely describes that authentication is performed locally within the personal identifier device. This is different from Applicant's claim requirement of a master template derived from a user's biometric digital representation previously produced by a biometric component of the personal identifier device.

For example, Bolle describes a biometric measurer which measures the corresponding biometric associated with user 402. According to Bolle, check 412 is performed in the querying system as to whether or not the acquired biometric matches the transmitted template 406, and upon successful matching an authentication message is produced.[1] Thus, while Bolle does describes a portable device 404 to measure the biometric of user 402, the locally generated

[1] Bolle, Col. 5, Lines 5-12

digital representation of the Bolle device is used compared to template 406 in order to authenticate the user. Thus, Bolle does not suggest that the portable device 404 itself produces the original digital representation of the user 402 biometric, i.e., the master template. Thus, even if Moritzen were modified in view of Bolle, Applicant's claimed invention would not be achieved. There is no teaching or suggesting in either of the references, either singularly or in combination, of a portable personal identification device that includes a biometric component that generates a master template for subsequent use in authenticating users.

Further, with respect to independent claims 1, 9 and 17, the Examiner correctly recognized that neither Maritzen nor Bolle teach or suggest a personal digital identifier device that generates a private key and a public key pair and outputs the public key for transmission. Further, the Examiner correctly recognized that neither Martizen nor Bolle teach or suggest a personal digital identifier device that securely stores the private key and being configured for producing, using and generating the private key.

With respect to these elements of claims 1, 9 and 17, the Examiner relies on Etzel and suggests that it would be obvious to one of ordinary skill in the art to modify the personal identification device of Maritzen system to locally generate both a private and a public key pair and output the public key for transmission.

However, Etzel fails to describe or suggest incorporation of these elements in the manner proposed by the Examiner. In this regard, Applicants believe that the Examiner may be misinterpreting either the reference or the claimed invention. For example, Etzel describes a centralized data encryption key management system used within a video information delivery system 100 that provides Video On Demand (VOD) services to a plurality of subscribers. Etzel describes that a security module 30 generates program encryption keys for each video program and that the keys are not disclosed outside of the video information delivery system 100, i.e., the "head end."

Thus, the Examiner's reliance on the key generation "facility" in Etzel as a teaching or suggestion of generation of a public and a private key within a portable, personal identification device is erroneous and contrary to the teachings of Etzel.[2] More specifically, the generation of keys at the centralized video delivery system, as taught by Etzel, is consistent with the prior art

[2] Etzel, Col. 1, Lines 53-59

and entirely contrary to the portable personal digital identifier device that is capable of internally producing and storing private and public encryption keys as required by independent claims 1, 9 and 17.

Thus, even if one of ordinary skill in the art at the time of the invention were to modify the Maritzen system in view of the teachings of Bolle in further view of Etzel, the resulting system would require the generation of encryption keys at a centralized server, as clearly taught by Etzel. In such a system, presumably the public key would be provided to another location or device, such as the personal digital identifier device, for authentication. This is directly contrary to Applicants' claims that require that the personal digital identifier device itself internally generate both the public key and the private key and be configured for producing and using the private key.

With respect to independent claim 17, the teachings of Maritzen fail to suggest a variety of requirements within the claim. For example, the reference discloses that the fingerprint identity sample will be stored in the transaction device by the processing facility.[3] This is in contrast to the present invention where the personal digital identifier itself receives an input biometric of said user, produces a digital representation thereof, derives from said digital representation a master template, and securely maintains said master template in storage. Creating and storing the master template outside of the portable device, as taught by Maritzen, is in direct contrast to the requirements of claim 17.

Further, the teachings of Maritzen describe providing secure content from a vendor to the user upon authentication[4]; however, access to the computer network has already been granted prior to authentication in the reference. Therefore, permitting said authenticated user to access said computer network through said workstation, as required by Applicants' claim 17, provides improved network security not anticipated or suggested by the provided reference. Additionally, the Maritzen teaching provides no motivation for someone of ordinary skill in the art to require authentication in order to access the network or workstation.

In regard to claims 4 and 14, Etzel fails to disclose a personal digital identifier device wherein all data held in said secure storage is by itself non-identifiable of said user. In rejecting

[3] Maritzen, Page 11, Paragraph 0143
[4] Maritzen, Fig. 17, No. 13

claims 4 and 14, the Examiner merely refers to a portion of Etzel that describes the facility (i.e., the central Video On Demand system) securely maintaining keys. While the reference teaches the encryption of data for secure transmission, nowhere does the description provide motivation for the data to be itself non-identifiable of said user. In fact, the keys of the Etzel system aren't even assigned to "users." Rather, the keys are used for encrypting video programs. Thus, the Examiner's reasoning with respect to claims 4 and 14 is difficult to understand. It appears the Examiner has overlooked or misunderstood Applicant's requirements that the data be "non-identifiable" of the user.

With regard to claim 15, Maritzen fails to suggest a security system wherein said network storage includes data identifiable of said user for display on a screen of said workstation when said user's personal identification device is located within said envelope. The cited portion of Maritzen discloses that secure distribution of physical (or electronic) content to the user is performed once the transaction is authorized.[5] However, this information is neither identifiable of said user nor displayed when said user's personal identification device is located within said envelope.

Similar to claim 15, claim 20 requires displaying on a screen of said workstation data identifying said user when said user is identified. Maritzen fails to teach these elements as data identifying said user is not displayed by the Maritzen system. Maritzen describes an on-screen icon, but this icon is generic to a digital wallet representative of any user performing a shopping activity.[6] Therefore, the on-screen icon fails to identify the user as such, and no motivation for an icon identifying the user is disclosed.

With regard to claim 22, Rydbeck fails to suggest that a policy manager component may direct that the screen of said workstation be blanked out when a new personal digital identifier device moves to a location within said envelope until such time as the user registered to said personal digital identifier device is biometrically identified.

In general, Rydbeck describes a method for automatically establishing a wireless link between a wireless modem and a communication device. In rejecting Applicants' claim 22, the Examiner states:

---

[5] Maritzen, Page 16, Paragraph 0210
[6] Maritzen, Page 15, Paragraph 0202

> Rydbeck discloses a communication device and a wireless device determining whether an electronic message is to be transferred by checking the elapsed time and sending a paging signal to the wireless device and if the wireless device is not responding to the signal, the wireless device returns to the standby state or not activated to transfer message.

Although this may be true, the functions described by the Examiner are completely irrelevant to Applicants' claim 22. Applicants' claim 22 requires a policy manager component that directs the screen of a workstation to be blanked out after a new personal digital identifier device is sensed until such time as the user registered to said personal digital identifier device is biometrically identified. In contrast, the Examiner seems to be describing functions for determining whether or not a device is even present.

For example, Rydbeck states if the phone 300 has responded to the page signal, then the method moves from step 630 to step 635 where the link is activated between the computer 100 and the phone 300.[7] Applicants believe that the Examiner is misinterpreting either the applied reference or the claimed invention. While Rydbeck does suggest a communication link between two devices, the disclosure does not suggest said workstation be blanked out when a new personal digital identifier device moves to a location within said envelope, as required by claim 22. In contrast, Rydbeck described activating a communication link upon detecting the device.

Dependent claims 2-3, 5-8, 10-11, 13, 19 and 21 are allowable for at least the reasons set forth above.

For at least these reasons, the Examiner has failed to establish a prima facie case for non-patentability of Applicant's claims under 35 U.S.C. 103(a). Withdrawal of this rejection is requested.

---

[7]Rydbeck, Col. 6, Lines 60-63

CONCLUSION

All claims in this application are in condition for allowance. Applicant respectfully requests reconsideration and prompt allowance of all pending claims. Please charge any additional fees or credit any overpayment to deposit account number 50-1778. The Examiner is invited to telephone the below-signed attorney to discuss this application.

Date: May 17, 2005

By: Kent J. Sieffert

SHUMAKER & SIEFFERT, P.A.
8425 Seasons Parkway, Suite 105
St. Paul, Minnesota 55125
Telephone: 651.735.1100
Facsimile: 651.735.1102

Name: Kent J. Sieffert
Reg. No.: 41,312